

### **REMARKS**

Reconsideration and allowance of the subject patent application are respectfully requested.

Claim 1, 3-6 and 13 were rejected under 35 U.S.C. Section 101 as allegedly being directed to non-statutory subject matter. Claims 1 and 13 are each amended to recite that the system is implemented on a computer apparatus to clarify that claims 1 and 13, and hence also claims 3-6 by virtue of their respective dependencies on claim 1, define hardware and so fall within the statutory category of patentable subject matter under 35 U.S.C. Section 101 of a machine. In this regard, Applicant notes that the detailed description beginning on page 2 describes a non-limiting, example embodiment which is shown in Figure 1. A person of ordinary skill reading this detailed description readily recognizes and understands that the example system 100 is implemented by a hardware computer apparatus.

Claims 1, 3-7 and 9-13 were rejected under 35 U.S.C. Section 103(a) as allegedly being made obvious by Roberts et al. (US 2004/0088570) and Bates et al. (US 6,721,721).

While not acquiescing in this rejection or in the characterizations of the applied references made in the office action, independent claims 1, 7 and 13 have now been amended to clarify the nature of the factor regarding the length of time, specifying that this factor is "the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe." This amendment has basis in the detailed description at, for example, page 3, lines 1-12 which sets out how the length of time is used as a factor to determine whether the file can be regarded as safe. This passage clearly explains that file which have been known for a longer length of time are more likely to be safe on the basis that any malware contained in the file will be more likely to have been detected, because the longer the time that passes the more likely it is that a file containing malware will have been submitted to the developers of a scanner who will have analyzed the file and updated their scanner to detect it.

At least taking into account this amendment, the rejection based on the proposed combination of Roberts et al. and Bates et al. does not apply for the following reasons. The

discussion below makes specific reference to claim 1, but similar reasoning applies to claims 7 and 13 which define similar features.

The office action acknowledges that Roberts et al. does not disclose the use of a factor of “length of time which the database indicates that the file has been known without malware containing instances of it being detected.” 1/16/2009 office action, page 7. However, the office action contends that this “length of time” feature is known from Bates et al. and that it is obvious to apply the relevant disclosure of Bates et al. to the disclosure of Roberts et al. to arrive at the claimed subject matter. Applicant respectfully disagrees with this argumentation.

Firstly, at least taking into account the amendment now made to claim 1, Bates et al. does not disclose the “length of time” feature that is acknowledged to be lacking in Roberts et al. In particular, claim 1 as now amended explicitly requires a factor of “the longer the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected the more likely that the file is safe.” In contrast, the office action relies on the disclosure in Bates et al. relating to block 98 of Figure 3. This relates to a “good URL threshold time” and is a step that is reached if it has been determined that an URL (1) has not changed since it was last virus checked (block 82) and (2) has been virus checked in the past and not been found to contain a virus (blocks 84 and 96). The effect of block 98 is that the web crawler submits the URL for virus checking when the good URL threshold time has elapsed, but does not submit the URL for virus checking when the good URL threshold time has not elapsed. In other words, additional virus checking is performed when a long period of time has elapsed since the URL was last virus checked and found to be safe. This corresponds to a factor of the longer the length of time the less likely that the file is safe.

Thus, Bates et al. does not disclose the feature of claim 1 that is lacking in Roberts et al. as set out above. Consequently, even if it would have been obvious to apply this feature of Bates et al. to the system of Roberts et al., the result would not be the system of claim 1.

Secondly, Applicant does not admit or agree that it would have been obvious to apply the disclosure of Bates et al. to Roberts et al. and nothing in these remarks should be viewed as acquiescence by the Applicant in this regard. However, it is not necessary to address this point inasmuch as, as noted above, Bates et al. fails to remedy the acknowledged deficiency of Roberts et al. with respect to the “length of time” feature.

SHIPP, A.  
Serial No. 10/500,957  
Response to Office Action dated January 16, 2009

The dependent claims distinguish from the proposed Roberts et al.-Bates et al. combination at least by virtue of their respective dependencies from one of claims 1 and 7.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By:                     /Michael J. Shea/                      
Michael J. Shea  
Reg. No. 34,725

MJS:mjs  
901 North Glebe Road, 11th Floor  
Arlington, VA 22203-1808  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100